陈至栩, 陈亮. 基于量化值算法的网络安全事件态势指标评估体系建设初探[J]. 智能计算机与应用,2025,15(6):196-201. DOI:10.20169/j.issn.2095-2163.24122801

基于量化值算法的网络安全事件态势指标评估体系建设初探

陈至栩, 陈 亮
(国家计算机网络应急技术处理协调中心贵州分中心, 贵阳 550001)

摘 要: 随着网络安全领域新技术融入和规模不断扩大,网络安全防护形势越发严峻。面向跨区域多分支的省市级网络安全问题,建立合理有效的态势指标评估体系,有助于以全局视角,系统、客观、科学了解和发现相关问题的发展现状及变化趋势。本文面向多种高发网络安全事件的多个细分领域,如受控主机数量、网页篡改事件、网站后门事件、CNVD 漏洞数量等,依照客观、全面、可操作原则,构建了一套由 4 个一级指标、17 个二级指标组成的网络安全事件态势指标评估体系,并将指标层次加权递归和 LOG 函数有机结合,设计了一种适用于网络安全事件态势评估的算法。实验证明,该设计符合网络安全态势分析客观规律,能够有效提升网络安全风险感知能力,促进网络安全治理管理水平。

关键词: 网络安全; 态势评估; 指标体系; 风险感知; 恶意程序
中图分类号: TP393.0 **文献标志码**: A **文章编号**: 2095-2163(2025)06-0196-06

Construction of network security events situation index evaluation system based on quantized value algorithm

CHEN Zhixu, CHEN Liang
(National Computer Network Emergency Technical Response Coordination Center/Guizhou Branch Center, Guiyang 550001, China)

Abstract: With the integration of new technologies in the field of network security and the continuous expansion of the scale, the situation of network security protection is becoming more and more serious. Facing the cross-regional and multi-branch provincial and municipal network security problems, the establishment of a reasonable and effective situation indicator evaluation system is conducive to systematically, objectively and scientifically understanding and discovering the development status and changing trend of related problems from a global perspective. Based on the objective, comprehensive and operable principles, this paper constructs a network security incident situation index evaluation system consisting of 4 first-level indicators and 17 second-level indicators for multiple subdivisions of a variety of high-incidence network security incidents, such as the number of controlled hosts, webpage tampering incidents, website backdoor incidents, CNVD vulnerabilities, etc. By combining index level weighted recursion with LOG function, an algorithm suitable for network security event situation assessment is designed. The experiment proves that the design conforms to the objective law of network security situation analysis, can effectively improve the ability of network security risk perception, and promote the level of network security governance and management.

Key words: security; situation assessment; index system; risk perception; malicious program

0 引 言

在万物互联的浪潮推动下,网络空间安全已经成为继海、陆、空、天之外人类活动的“第五空间”。网络安全是总体国家安全观的重要组成部分,关乎国家安全、经济社会稳定运行以及广大人民群众的切实利益。随着《网络安全法》、《数据安全法》等法律相继颁布实施,国内系统构建了网络空间法律法规体系,有效防范化解网络安全风险,进一步增强网络安全防御能力[1]。但是同时也应该清醒地认识到,近几年来出现的网络安全问题内因在于仍然缺乏有效的管理方式和思路,评价指标体系不统一,导致具体措施落实不到位,进而形成网络安全问题恶性循环[2]。因此,不应该盲目追求大规模安全投入和有效性不清晰的安全建设,而是要恪守最低有效洞察力(Minimum Effective Insight)原则[3],根据实际拥有的资源和能力,合理决策对安全控制措施的部署和使用。因此,在开展网络安全能力建设时,构

作者简介: 陈至栩(1996—),男,硕士,初级工程师,主要研究方向:网络安全态势评估体系建设。Email:836105052@qq.com。

收稿日期: 2024-12-28

建一套能够进行客观评价的指标体系，对于把握某项工作总体网络安全态势变化情况具有重要意义，有利于将评价指标体系与安全防护工作目标紧密联系[4]。本文基于量化值算法构建了一套客观、全面的网络安全态势指标评估体系，希望能够为监测网络安全事件、发现网络安全态势运行规律提供一定的理论支撑。

1　网络安全事件态势指标评估体系基本概念

态势指标评估体系设计是为对当前和未来网络安全运行状态进行评估预判，对网络安全态势运行客观规律进行探索，是网络安全态势研究工作的基础内容之一[5]，因此在指标选取、指标定义、权重赋值判断等方面存在一定的复杂性，主要体现在以下 4 个方面：

（1）指标选取较少，导致态势评估不完整，选取较多导致存在冗余指标，造成数据采集工作量增加。

（2）完全依赖人为主观判断进行指标选取，可能造成部分指标被忽略，导致评估体系难以全面体现网络安全态势情况。

（3）指标定义不精准，可能造成不同指标之间存在关联，影响态势指标评估结果发生偏移。

（4）权重赋值不准确或不根据现实情况进行动态调整，则会导致态势评估效率降低[6]。

基于上述几类复杂性问题，网络安全事件态势指标评估体系需要充分进行调查研究和监测分析，对各项指标选取和定义进行认真评估，依据事件监测实际情况对权重赋值进行动态调整，才能更加准确地掌握某一地区网络安全态势变化情况[7]。

目前，层次分析法是获得广泛应用的指标评估方法[8]。针对复杂的多目标决策问题，首先将其视为一个整体系统，随后将总体目标细分为若干个子目标或准则，并进一步分解为多层次的多指标，通过运用定性指标的模糊量化技术，计算各层次的单一排序及综合排序，从而为实现多指标、多方案的优化决策提供科学依据[9]。

1.1　指标概念

指标用于阐述总体的综合数量特征，由名称与数值两个要素构成，展现了事物在质与量两个维度上的规定性特征[10]。在统计学中，指标是用来描述和衡量某一现象的数量特征的工具，如工业普查中的企业、职工总体数量、以及工资总额等，都是用来反映总体数量特征的指标。指标亦可定义为评估目标达成度的参数、预期的指数、规定的规格或标准，通常以数据形式来进行具体量化[11]。例如，在商业和股市分析中，技术指标是通过数学模型和计算公式得出的数字，这些数字反映了市场的某个内在实质，为操作行为提供指导方向[12]。综上所述，指标的基本内涵不仅限于统计学中的概念，同时还扩展到更广泛的领域、如商业和股市分析中，通过数学模型和计算公式得出结果数字，这些数字反映了市场的内在实质，为决策提供依据[13]。

1.2　态势指标评估体系设计原则

从系统视角出发，指标体系构建了一个对研究对象进行抽象与刻画的概念框架，用以综合量化描述总体的基本状况及各变量的分布特性。研究中依据设计的指标及计量结果，旨在揭示或验证研究对象的实际状况[14]。指标体系设计应遵循以下 6 个原则。

（1）系统性原则：凸显层次性是指标体系构建的特点之一，各指标之间相互独立又彼此联系，存在相应的逻辑关系，一组指标构成一个子系统，形成一个有机统一体。

（2）典型性原则：评价指标需具备典型性，以便精确映射特定区域相关问题的整体特征。即便在指标数量适度缩减时，也应确保后续数据运算，从而提升结果的可信度。

（3）动态性原则：一定的时间尺度是反映出指标体系研究问题实质内涵的重要因素。因此，指标的选择应以若干年度的动态变化数值为准。

（4）简明科学性原则：指标体系的设计必须以科学性为原则，计算方法简明易懂，为真实展现各指标间的内在联系，所选指标应兼具代表性和典型性。指标数量不宜冗杂繁复，以免重叠混淆；同时，也不可过于简略，以防信息缺失，导致结论失真或产生误导。

（5）可比、可操作、可量化原则：所选指标需具备简明性、微观针对性，以及实际的可操作性和可比较性。在选取指标时，需考量其是否便于量化处理，从而有利于数学运算与分析。尤为重要的是，在整体研究范畴内，指标的计量标准和计算方法必须保持统一。

（6）综合性原则：在相应的评价层次上，全面考虑影响指标体系整体系统的诸多因素，并进行综合分析和评价。

2　基于量化值算法的网络安全事件态势指标评估体系设计

网络安全事件态势指标评估体系主要包括指标要素、指标权重、量化值、态势指数等四个部分。

2.1 指标要素和权重

指标要素用于说明每个指标的具体类别,可基于类别重要性定义指标级别,指标权重是对每个指标项赋予一个参考数值,通过数值反映指标相对重要程度,对不适用于评价指标体系工作的部分指标,将权重赋值为 0 或不纳入指标体系中[15]。本文针对 A 省监测发现的网络安全事件特点,结合分析事件造成的影响筛选出重要因素,按照一定准则对部分一级指标进行分析分解,针对性地设计了多个二级指标及相应权重。4 个一级指标分别是:受控主机数量、网页篡改事件、网站后门事件、CNVD 漏洞指数,其一级权重分别为:0.4、0.2、0.2、0.2,一级指标权重总和为 1,各一级指标下的二级指标权重总和为 1。权重不因指标统计数量变化而变化,但会随着指标评估体系的不断完善,指标划分更加精准,权重也会进行相应调整。

本文用 R 表示一级指标,Z 表示一级权重值,r 表示二级指标,z 表示二级权重值。网络安全态势指标评估体系设计框架如图 1 所示。各项一级指标权重设置见表 1。

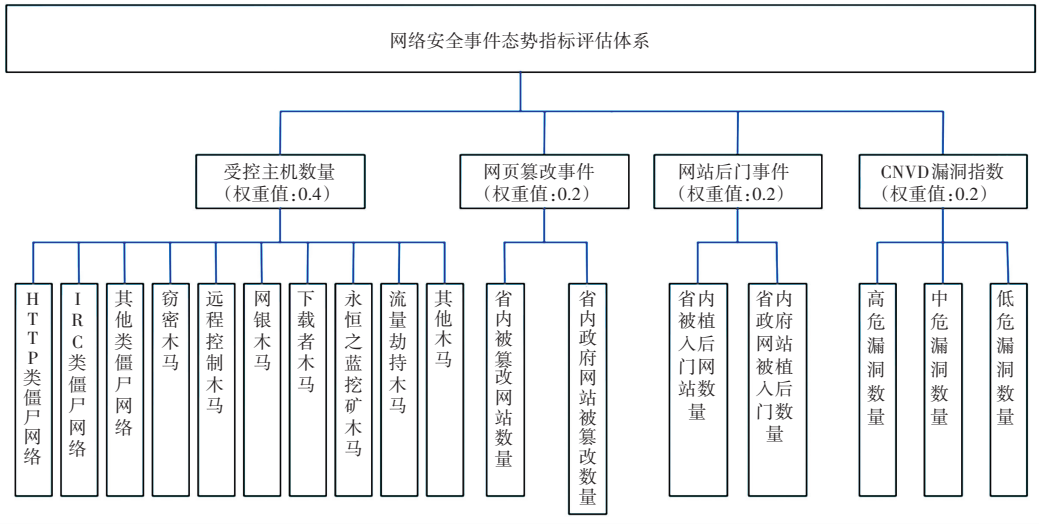

图 1 网络安全事件态势指标评估体系框架图

Fig. 1 Block diagram of network security events situation index evaluation system

表 1 一级指标及对应权重

Table 1 First level index and corresponding weight

一级指标名称	一级权重
$R1$: 受控主机数量	$Z1$: 0.4
$R2$: 网页篡改事件	$Z2$: 0.2
$R3$: 网站后门事件	$Z3$: 0.2
$R4$: CNVD 漏洞指数	$Z4$: 0.2

2.1.1 受控主机数量指标

受控主机数量指标注重于反映某一地区恶意程序事件态势变化状况[16]。网络安全事件中的恶意程序事件,涉及蓄意创建并散播有害程序,或由此类程序引发的安全问题。有害程序、即被非法植入信息系统的代码段,会对系统数据的保密性、完整性和可用性构成威胁,或干扰系统的正常运行[17]。该类别下细分为计算机病毒、蠕虫、特洛伊木马、僵尸网络、混合攻击程序、网页嵌入恶意代码及其他有害程序等 7 项子类别。近年来,恶意程序事件的多样性和数量均呈上升趋势,导致其在特定时段内的态势预测变得更加复杂和不确定。

受控主机数量指标为本设计中占比较大的一级指标,通过收集和预处理受控主机数量等相关数据进行态势指标评估,对该指标进行分解设计的思路主要考虑恶意程序控制主机的两大因素:僵尸网络和木马病毒。其中,僵尸网络是指利用僵尸工具软件,形成僵尸网络而引发的一类网络安全事件,在此类事件中,黑客集中操控的计算机群、即僵尸机器,可被用于策划网络攻击、窃取敏感信息,或散布木马、蠕虫等恶意程序。木马病毒是用于远程控制计算机的病毒程序,将控制程序寄生于被控计算机系统中,通过内外配合对被受害计算机实施监控、篡改等操作[18]。受控主机数量指标的二级指标主要包括 HTTP 类僵尸网络、IRC 类僵尸网络、其他僵尸网络、窃密木马、远程控制木马、蠕虫木马、下载者木马、挖矿木马、APT 木马、其他木马等 10 个二级指标。该分类下的二级指标权重设置见表 2。

表 2　受控主机数量指标及其对应权重

Table 2　Controlled hosts index and corresponding weight

指标名称	二级权重
$r1$：HTTP 类僵尸网络	$z1$：0.175
$r2$：IRC 类僵尸网络	$z2$：0.175
$r3$：其他僵尸网络	$z3$：0.165
$r4$：窃密木马	$z4$：0.055
$r5$：远程控制木马	$z5$：0.125
$r6$：蠕虫木马	$z6$：0.025
$r7$：下载者木马	$z7$：0.125
$r8$：挖矿木马	$z8$：0.030
$r9$：APT 木马	$z9$：0.025
$r10$：其他木马	$z10$：0.100

2.1.2　网页篡改事件指标

网页篡改是黑客利用技术手段对网站上传网页木马，获取控制权限后对网页内容进行恶意篡改操作，具有传播速度快、阅读人群多、影响范围大、消除影响难、预先检查和实时防范难等特点，是一种成本较低、但是危害较大的黑客手段[19]。本文对网页篡改事件指标下进行分解设计，主要包括 A 省被篡改网站事件数量和 A 省政府网站被篡改数量等 2 个二级指标。该分类下的二级指标权重设置见表 3。

表 3　网页篡改事件指标及其对应权重

Table 3　Web tampering index and corresponding weight

指标名称	二级权重
$r11$：A 省被篡改网站数量	$z11$：0.4
$r12$：A 省政府网站被篡改数量	$z12$：0.6

2.1.3　网站后门事件指标

网站后门是黑客或不法开发者在网站系统中故意植入的一段代码或机制，可以绕过正常的认证机制，长期维持对网站的控制权，以便日后能够未经授权再次秘密进入系统，执行非法操作或窃取数据，是一种可能造成长期性危害的黑客手段[20]。本文对网站后门事件指标进行分解设计，主要包括 A 省被植入后门网站数量和 A 省政府网站被植入后门数量两个二级指标。该分类下各项二级指标权重设置见表 4。

表 4　网站后门事件指标及其对应权重

Table 4　Website backdoor index and corresponding weight

指标名称	二级权重
$r13$：A 省被植入后门网站数量	$z13$：0.4
$r14$：A 省政府网站被植入后门数量	$z14$：0.6

2.1.4　CNVD 漏洞发现指标

对涉及 A 省的 CNVD 漏洞发现数量按照危害级别进行分解设计，其二级指标主要包括：高危漏洞数量、中危漏洞数量、低危漏洞数量。该分类下的二级指标权重设置见表 5。

表 5　CNVD 漏洞发现指标及其对应权重

Table 5　CNVD vulnerability found index and corresponding weight

指标名称	二级权重
$r15$：高危漏洞数量	$z15$：0.5
$r16$：中危漏洞数量	$z16$：0.3
$r17$：低危漏洞数量	$z17$：0.2

2.2　量化值和态势指数

一般评价指标的量化值运算主要基于定量分析法的 5 种基本方法：比率分析法、趋势分析法、结构分析法、相互对比法和数学模型法。本研究通过监测发现各类型恶意程序事件数量、网页篡改事件数量、网站后门事件数量、CNVD 漏洞发现数量采用数学模型法对各项指标的可量化数据进行分析，并对整体态势进行评价，提出一种基于对数函数的指标评估体系算法，其量化值 α 数学计算式为：

$$\alpha = 100 \times \frac{\log_{10}\sigma - \log_{10}\varepsilon}{\log_{10}\partial - \log_{10}\varepsilon} \tag{1}$$

其中，σ 表示各项二级指标当前统计值；∂ 表示各项二级指标历史统计数据中的最大值；ε 表示各项二级指标历史统计数据中的最小值，其数学定义式则为：

$$N = 100 \times \frac{\log_{10}(N_C) - \log_{10}(N_{\min})}{\log_{10}(N_{\max}) - \log_{10}(N_{\min})} \tag{2}$$

其中，N 表示量化值；N_C 表示当前统计值；$N_{\max}$ 表示最大值；$N_{\min}$ 表示最小值。

基于量化值 α 计算的态势指数 φ 数学定义式为：

$$\varphi = 100 - [(\alpha_{r1} \times z1 + \cdots + \alpha_{r10} \times z10) \times R1 + (\alpha_{r11} \times z11 + \alpha_{r12} \times z12) \times R2 + (\alpha_{r13} \times z13 + \alpha_{r14} \times z14) \times R3 + (\alpha_{r15} \times z15 + \cdots + \alpha_{r17} \times z17) \times R4] \tag{3}$$

3　网络安全事件态势指标评估体系实现

依据建立的指标评估体系和算法设计，整个指标评估体系的实现包括指标数据采集、指标统计、指标计算和可视化呈现。指标数据采集主要负责收集与指标体系相关的原始数据，包括僵尸网络、木马病毒等事件数量，对所有原始数据按照指标体系量化

值算法设计进行运算,得到标准量化值,在量化数据结果基础上根据不同的维度指标调用相应的权重,按态势指数算法得到最终指数结果。

本指标体系设计以周为单位进行指数统计(即 7 天为 1 个周期),当态势指数 $\varphi \leqslant 60$ 时、即代表本周态势评估结果较差,造成这一结果的原因可能是各类网络安全事件频繁发生,各维度扣分指标较多;当 $60 \leqslant \varphi \leqslant 80$ 时,代表本周态势评估结果为中,网络安全事件发生频率较高,部分维度各项指标可能与其他指标形成明显差异;当 $80 \leqslant \varphi \leqslant 90$ 时,代表本周态势评估结果为良;当 $\varphi \geqslant 90$ 时,代表本周态势评估结果为优。当态势评估结果为良或优时,可对突出扣分指标相应的网络安全问题进行溯源分析,定期开展专项网络安全检查。

计算出所有指标的态势指数后,可综合受控主机、网页篡改事件、网站后门、CNVD 漏洞数量等一级指标将相关态势指数和量化值进行可视化呈现,帮助相关行业监测人员全面掌握网络安全态势变化,优化管理措施,针对性开展网络安全专项检查、应急演练,在网络安全竞赛中设计特定考题,加强相关行业人员应急处置能力。

依照本文提出的基于量化值算法的网络安全事件态势指标评估体系,尝试对 A 省半年内的监测数据进行采集测试,其态势评估波动如图 2 所示。由图 2 可以看出,A 省在 2023 年上半年的网络安全态势指数处于 80~90 分区间波动,虽然存在起伏、但是整体态势评估结果总体为良,少数几周为优,可推断出 A 省在这一时间范围内的网络安全态势总体可控,未发生较大网络安全事件。根据分数结果,可针对态势指数相对较低的时间段,分析各项指标具体分数情况,开展网络安全专项排查并进行针对性的整改。

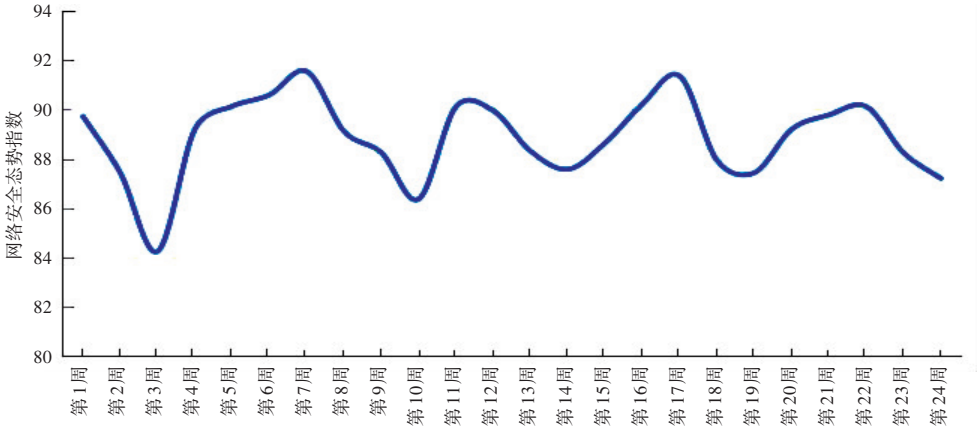

图 2 A 省 2023 年上半年网络安全态势变化图

Fig. 2 Network security situation change map of A province in the first half of 2023

4 结束语

本文针对网络安全事件中的多个细分领域,按照层次分析法和指标评估体系设计原则,结合层次加权递归、LOG 函数设计量化值和态势指数算法模型,提出一种基于量化值算法的网络安全事件态势指标评估体系,并将这一体系和评估模型应用到实际工作中。实践表明,能够帮助相关行业工作人员掌握某一地区网络安全态势变化。在未来的工作中,还需充分掌握各地区、各行业网络安全态势情况,从事件监测、权重调整、算法优化、覆盖面扩大等方面持续不断完善态势指标评估体系建设。

参考文献

[1] 李云峰,张红历,夏怡凡,等. 关基单位网络安全能力评价指标体系研究[J]. 信息安全与通信保密,2023(5):68-80.

[2] Good Firms. ODM:一种以结果为导向的网络安全建设度量指标体系 [EB/OL]. (2025-04-02). https://10xds.com/blog/why-and-how-of-outcome-driven-security-metrics/.

[3] CHENG Xiaorong, LANG Su. Research on network security situation assessment and prediction [C]//Proceedings of 2012 Fourth International Conference on Computational and Information Sciences. Piscataway,NJ:IEEE,2012:864-867.

[4] 李军,黄健,朱豪杰. 内部网络安全监管指标体系设计与实现[J]. 通信技术,2022,55(2): 241-246.

[5] 魏军,公伟,肖扬文,等. 信息安全监管工作评价指标设计浅谈[J]. 信息安全与通信保密, 2017(10):35-41.

[6] 刘佩雯. 数字经济时代网络安全产业评价指标体系研究[J]. 网络安全技术与应用, 2024(7):94-96.

[7] 张卓群. 中国网络安全产业发展态势及对策研究[J]. 北京工业大学学报(社会科学版),2022,22(3):75-85.

[8] 薛钰,周锦,杨秉杰. 僵尸木马控制事件的最优研判条件选择方法[J]. 网络安全技术与应用,2024(2):36-39.

[9] 刘静. 基于泛在网络的安全事件描述与风险分析研究[J]. 中国新通信,2023,25(18):107-109.

[10]李蒙. 新形势下网络安全事件应急管理研究[D]. 重庆:重庆大学,2021.
[11]王茂忠. 信息网络安全事件监测与响应平台的设计[J]. 电子技术,2020,49(11):116-117.
[12]董良遇,赵冉. 我国工业信息安全态势分析与思考[J]. 信息技术与网络安全, 2019, 38 (12):37-41.
[13]李璐璐. 大数据及人工智能技术的计算机网络安全防御系统研究[J]. 网络安全技术与应用,2024(6):24-26.
[14]马龙. 基于免疫浓度的网络安全态势感知评估方法研究[D]. 西安:西安邮电大学,2017
[15]李茹,翟书颖,智永锋. 面向中小型企业的态势感知体系研究[J]. 现代电子技术,2021,44(9):83-87.
[16]LI Zhengmao, MA Tingting, ZHOU Yanling, et al. Research and simulation of network security situation prediction algorithm[J]. Journal of Physics: Conference Series,2021,1941(1):012051.
[17]CHEN Xiyue, PANG Jianmin. Temporal logic-based artificial immune system for intrusion detection [J]. Wireless Communications and Mobile Computing,2022(1):1-9.
[18]CHANG Liwei, LIU Xiujuan, QIAN Yuhua, et al. Network security situation awareness model based on multi-source fusion of convolutional neural networks[J]. Computer Science, 2023, 50 (5): 382-389.
[19]WANG Yixuan, ZHAO Bo, LI Weidong, et al. An ontology centric approach for network security situation awareness[C]// Proceedings of 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC). Piscataway, NJ: IEEE, 2023: 777-787.
[20]ZHAO Dongmei, SHEN Pengcheng, ZENG Shuiguang. ALSNAP:Attention-based long and short-period network security situation prediction[J]. Ad Hoc Networks, 2023, 150: 103279.